Privacy

- What are privacy concerns?
- Why is privacy important?
- How does cybertechnology impact privacy?
- How do we protect privacy?
• General privacy concerns involving cybertechology impact everyone, regardless of computer use

• Are cyberprivacy concerns unique or special?
  – not new, but aggravated
  – technology has affected
    * accuracy and amount of information
    * speed of transmission
    * length of retention
    * kind of information that can be transmitted
What is privacy?

- repository of personal information can be diminished
- a spatial zone can be invaded
- confidentiality or trust can be violated

Distinguish having privacy (descriptive) from having a right to privacy (normative)
Three views of privacy

- **Freedom from intrusion**
  - 1890 first explicit reference as a legal right
  - prompted by the use of cameras
  - may be implied by Fourth Amendment (protection from unreasonable searches and seizures)

- **Freedom from interference in personal affairs**
  - decisional privacy
  - right not to be interfered with
  - contraception, abortion, right to die, euthanasia

- **Access and control of personal information**
  - informational privacy
  - who has access to personal information?
  - to what extent can an individual control the ways in which information can be gathered, stored, mined, combined, exchanged or sold?
An individual has privacy in a situation if he is protected from intrusion, interference, and information access by others.

Differentiate between a loss of privacy and a violation of privacy.

- hiking alone in the woods
  - no expectation or right to privacy
  - privacy can be lost but not violated

- surveillance camera hidden in a dorm room
  - privacy is protected by laws or policies
  - privacy is violated
Privacy as a Value

- not a universal value
- problem for laws and policies in cyberspace
- necessary means to trust and friendship (more than instrumental)
- desired for its own sake? no.
- expression of the core value security
- essential for autonomy, freedom and independence
- provides social value – necessary for democracy
Data Gathering

- not new

- cybertech allows it without the knowledge and consent of the person

- data monitoring and recording
  - wiretapping, store video cameras, tollbooth scanners
  - workplace monitoring, website monitoring, "click-streams"

- cookies
  - information is gathered and stored on user’s computer without his knowledge
  - information can be combined from multiple sources
  - defense: cookies can be disabled
  - default is to accept
- RFID tags
  - microchip + reader
  - intended to ID objects and track inventory
  - can monitor after sale
  - autos, clothing, cattle, dogs, humans
  - Bill of Rights
    * know if product contains tags
    * have tags removed or disabled on purchase
    * know when, where, and why tags are being read

- government surveillance
  - domestic syping
  - threat to privacy and civil liberty
  - gps chips mandated in cell phones since 2005
  - monitor email
  - subpoena records of online search requests
  - also used to combat crime and terrorism
  - issues of privacy and civil liberty
Merging and Matching Records

- collection, exchange and sale of personal data violates privacy
- merging is the technique of extracting information from two or more unrelated databases and integrating information
- giving information to an organization is not violation of privacy
  - merging multiple sets of information without consent is a violation
- matching is cross checking records in two or more unrelated databases for matches or hits.
- used to produce lists of potential lawbreakers
- problem: match the innocent as well as the guilty
- information is given to each database with consent, but matching is done without consent
Data Mining

- indirect gathering of personal information through an analysis of implicit patterns discoverable in data
- can generate new, non-obvious classifications to which and individual can be linked
- no legal protection with respect to how this information can be used
- raises special concerns
- threat to privacy
- laws and informal guidelines protect information that is explicit, confidential and exchanged among databases. Information extracted by data mining may be none of these.
Personal Information in Public

- personal data exists in databases and can be merged, matched or mined – not public
- personal data can be mined from internet transactions and webpages – public
- should there be legal protection for public personal data?
- search engines and privacy
  - each request is logged
  - users can gather information about people
- public records are often online or are sold and placed online
  should governments sell data?
Privacy Enhancing Tools

- protect privacy and personal information of users engaged on online activities
- compromise between legislation and industry self-regulation
- email encryption, Anonymizer.com, trust marks
- issues of consumer education, informed consent, and social equity

Legislation and Industry Self-Regulation

- W3C – Platform for Privacy Preferences
- TRUSTe – trust engine
- 1974 Privacy Act
- 2003 HIPAA – medical only
- Patriot Act
- FISA
- EU Directive on Data Protection